Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0831-V7-2023

for

SMGW Version 2.1

from

Power Plus Communications AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0831-V7-2023 (*)

Smart Meter Gateway

SMGW
Version 2.1

from	Power Plus Communications AG
PP Conformance:	Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2 and AVA_VAN.5
valid until:	10 December 2031

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5 as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 11 December 2023

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Sandro Amendola L.S.
Director-General

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

4 Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the component AVA_VAN.5 that is not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product SMGW, Version 2.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0831-V5-2022. Specific results from the evaluation process BSI-DSZ-CC-0831-V5-2022 were re-used.

The evaluation of the product SMGW, Version 2.1 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 1 December 2023. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Power Plus Communications AG.

The product was developed by: Power Plus Communications AG.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 11 December 2023 is valid until 10 December 2031. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.
4. to monitor the resistance of the certified product against new attack methods and to provide a positive qualified confirmation by applying for a re-certification or re-assessment process on a regular basis every two years starting from the issuance of the certificate.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product SMGW, Version 2.1 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Power Plus Communications AG
Dudenstraße 6
68167 Mannheim

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the “SMGW Version 2.1” consisting of the “SMGW Software”, Version 2.2.0 and the “SMGW Hardware”, Version 2.0.

The Smart Meter Gateway (SMGW) is an electronic unit comprising hardware, software and firmware used for collection, storage and provision of meter data from one or more meters of one or multiple commodities.

The Gateway connects a wide area network (WAN) with a network of devices of one or more smart metering devices (local metrological network, LMN) and the consumer home area network (HAN), which hosts controllable local systems (CLS). The security functionality of the TOE comprises protection of confidentiality, authenticity, integrity of data and information flow control mainly to protect the privacy of consumers, to ensure a reliable billing process and to protect the smart metering system and a corresponding large scale infrastructure of the smart grid.

Besides a certified security module (product name “TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE”, BSI-DSZ-CC-0957-V2-2016), the hardware device “Smart Meter Gateway” also includes a hard-wired communication adapter which both are not part of the TOE but which are always inseparable parts of the delivered entity. This communication adapter can be either a BPL, an Ethernet, a G.hn, an LTE or an LTE450 communication adapter.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.2 to 6.10. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF.1: Authentication of Communication and Role Assignment for external entities	Authentication, confidentiality and integrity protection by TLS secured communication channels with external entities.
SF.2: Acceptance and Deposition of meter data, Encryption of meter data for WAN transmission	Reception of meter data from a paired meter via the LMN interface, storage of meter data in the filesystem of the TOE and transmission of meter data to external entities via the WAN interface is cryptographically protected from disclosure and manipulation.
SF.3: Administration, Configuration and SW Update	Administration and configuration as well as updating the TOE’s software by an authenticated Gateway Administrator (GWA).
SF.4: Displaying Consumption Data	Displaying consumption data to authenticated Consumers at interface IF_GW_CON
SF.5: Audit and Logging	Generation of audit data for all security relevant actions and storage of audit records in System-, Calibration- and

TOE Security Functionality	Addressed issue
	Consumer-Logfiles.
SF.6: TOE Integrity Protection	Detectable physical tampering through the TOE's sealed packaging of the device. TSF integrity protection by secure boot process and regular as well as on-demand self tests. Preservation of a secure state in case of failures.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1 to 7.6.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3 to 3.5.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

SMGW, Version 2.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SMGW Hardware (as built in part of the Smart Meter Gateway)	Version 2.0 (Value 2A in the hardware revision number)	Secure delivery process as described below this table
2	SW	SMGW Software	Version 2.2.0 identified by the value 00861-34788	Pre-installed on the HW or updated by the GWA
3	DOC	Handbuch für Verbraucher, Smart Meter Gateway [10]	Version 4.11 SHA-256: e24e25671d2c16224e058247eb5fdfbb1cfdf8bd89de2ee318f99f1f9e776beb	Personal handover by the developer or download from https secured website
4	DOC	Handbuch für Service-Techniker, Smart Meter Gateway [11]	Version 5.6 SHA-256: 9966741b00848419339c729cc6bfff6f7bed2ef348e681e0cb04122ece3865d6	Personal handover by the developer or download from https secured website
5	DOC	Handbuch für Hersteller von Smart-Meter Gateway- Administrations-Software, Smart Meter Gateway [12]	Version 4.13 SHA-256: 43f69e9458e582262a7d2505209e8b0233a4729854c906d4d29200eb92d70f30	Personal handover by the developer or download from https secured website
6	DOC	Logmeldungen, SMGW Version 1.3 & 2.1 & 2.1.1 [13]	Version 3.4 SHA-256: f3a935b6ae1713ccdaa02411b377377a8e4f7dfb092a181efe1a6c9a86f17a64	Personal handover by the developer or download from https secured website
7	DOC	Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung [14]	Version 1.4 SHA-256: 17e280428e1602759b7bfa7dbbfde2e8d65ad7d518a96f0ab41a7130a9f38205	Personal handover by the developer or download from https secured website

Table 2: Deliverables of the TOE

The main circuit board of the TOE is built into a sealed case of the complete product (Smart Meter Gateway) and can be identified by the laser engraving on the case showing the hardware revision number. The revision number follows the following structure: “SMGW-X-YY-111-n0”. Thereby the X stands for the communication variant (B=BPL, E=Ethernet, J/K=LTE, N=G.hn, V=LTE450). YY stands for the product generation and corresponds to the TOE hardware version (2A=Version 2.0). The n stands for the SIM card type (0=none, 1=SIM card assembled at factory and SIM slot, 2=SIM card assembled at factory only, 3=SIM slot only). For more details see ST [6], chapter 1.2.

The software part of the TOE consists of the operating system and the SMGW application. It can be identified by a two-parts value, which consists of two revision numbers of the underlying version control system for the TOE, where the first part stands for the operating system and the second part stands for the SMGW application.

The guidance documentation for the different user roles [10], [11], [12] explains how to retrieve the software version information from the TOE.

The certified delivery process considers the complete delivery, starting with the manufacturer, through the different stages of storages, to the final place of installation in the consumers premises.

In this standard delivery process the hardware parts are delivered within a special and secure transport box (pylocx box).

Deviant to the standard delivery process, a personal handover by two employees of the producer or developer is also allowed for up to ten devices. Details can be found in the guidance document [14].

The software is pre-installed on the hardware and therefore also part of the physical delivery. In case of a software update of an already installed SMGW, the certified software update package will be securely transmitted from the developer to the GWA, who will use the TOE update functions to install the new software version.

The guidance documents mentioned in table 2 can either be downloaded by an https secured website https://service.ppc-ag.de (standard delivery) or (in case of personal delivery) they will be personally given to the consumer. In case they are downloaded, they can be uniquely identified by checking the hash sum from table 2 above, which are also included in the Security Target [6], chapter 1.2.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:
Security audit, secure communication, cryptographic support, user data protection, identification and authentication, security management, privacy protection, protection of the TSF and trusted channels.

Specific details concerning the above mentioned security policies can be found in the Security Target [6], chapter 7.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Trustworthy authorised and authenticated external entities
- Trustworthy and well-trained Gateway Administrators and Service Technicians
- Basic level of physical protection by installation in a non-public environment within the premises of the consumer
- Processing Profiles are obtained from a trustworthy and reliable source only
- Usage of certified Security Module for specific cryptographic services
- Certification of firmware updates prior to installation in the SMGWs
- Reliability and availability of WAN network connections, trustworthiness and availability of time sources, assumptions on LMN and HAN network connections
- Secure generation of ECC key pair and secure transmission to SMGW by the GWA

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE consists of three subsystems called “Hardware”, “Betriebssystem” and “SMGW-Anwendung”.

The subsystem “Hardware” is the physical basement of the TOE and implements the electronic part as well as the case and seal of the device. It also offers the physical connection to other hardware parts (e.g. power circuit board, communication adapter) which are not in the scope of the TOE.

The subsystem “Betriebssystem” controls the hardware and manages the different bus systems, memory and the CPU. Furthermore, it provides the basic input/output functionality. Additionally, it sends and receives commands by using the physical interfaces of the hardware. The subsystem itself runs on a Linux-based kernel.

The main functions of the subsystem “SMGW-Anwendung” are to collect meter data from connected meters, internal processing and storage of the received meter data, sending the processed meter data to authorized external entities and the overall security management of the TOE.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

7.1. Test configuration

The tests in the context of the evaluation have been conducted using different software versions of the TOE (00852-34781 (release version 171), 00858-34786 (release version 172), final TOE software version 00861-34788 (release version 173)) that are functionally consistent with the version under evaluation as specified in the ST [6], chapter 1.2.

The ITSEF verified by source code analysis that neither the TOE behaviour, nor any further security-relevant effects might result by the performed source code adaptions. Furthermore some slightly modified TOE versions (e.g. a TOE with SSH capabilities) were used to enable detailed testing. For most of the test cases, the unmodified TOE was used. Only where necessary, the modified TOE configurations were used, demonstrably without influencing the tested security functionality.

The final test procedure with all independent and penetration tests was performed with firmware version 00861-34788, which is the final TOE version as stated in the ST [6].

7.2. Developer Testing

The developer's testing approach was to systematically test the TOE security functionality and the TSFI as well as the TOE behaviour on the level of the subsystems. Thereby all security functions as defined in the ST [6], chapter 7.1 – 7.6 have been tested. In order to do this, the developer selected a subset of more than 400 test cases of the tests that were produced during the development of the TOE, which was suitable to sufficiently cover the TSF.
All test results were as expected.

7.3. Independent and penetration testing

The evaluation body chose to broadly cover all existing TSFI without specific restrictions.

The evaluation body chose to repeat a defined subset of the developer tests with the intent to cover the existing interfaces and the implemented security functionality in order to verify the developer test results.

Independent and penetration tests of the evaluation body are mainly performed on stand-alone test equipment, containing approx. 3000 automated test cases in about 150 test suites developed by TÜVIT, partitioned according to the security functions defined in the ST [6], chapter 7.1 to 7.6. Using this environment, every necessary role with corresponding rights (Gateway Administrator, Service Technicians, Consumers) and meters might be emulated at the appropriate TSFI. In particular, for testing the TSFI for connecting meters, it contains a "meter simulator", which allows to emulate and connect multiple meters, controlling their behaviour (e.g. for inducing errors). Using a dedicated crypto proxy, it is further possible to extract the nested CMS data, supported by the enhanced Wireshark, which was enriched by the implementation of various dissectors.

In summary, all independent and penetration tests were deployed on the final TOE (SW version 00861-34788) by the ITSEF. Furthermore, all differences between the certified SW version of the TOE during the previous certification (BSI-DSZ-CC-0831-V5-2022) and the actual one under evaluation (BSI-DSZ-CC-0831-V7-2023) were analysed by detailed source code analyses without further indication of potential vulnerabilities.

The evaluation body conducted penetration testing based on functional areas of concern derived from SFRs and architectural mechanisms. The areas were prioritised with regard to various factors, e.g., attack surface, estimated flaw likelihood, developer testing coverage, detectability of flaws during developer testing. In summary, all security functionalities as well as all TSFIs were tested.

Medium and high areas were guaranteed to be penetration tested, with a stronger emphasis on high priorities. Low priorities were also considered during penetration, but could be less emphasised, if developer tests were found to be sufficient.

The penetration testing activities were performed as tests and as analytical tasks. Whenever an analysis was estimated to yield better results, the evaluators chose the analytical approach. Analytical activities were especially applied in the areas secure boot, self-protection, domain separation, kernel and system hardening as well as non-bypassability. Combined approaches were also applied.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE's operational environment provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE as identified in chapter 2 has been evaluated. The SMGW Version 2.1 consists of the “SMGW Software”, Version 2.2.0 and the “SMGW Hardware”, Version 2.0.

Note that there are no further configurations since the different variants of the communication adapter are outside of the TOE scope.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 [4] (AIS 34) and guidance specific for the technology of the product [4] (AIS 46, 48).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2 and AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0831-V5-2022, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on changes to the wMBUS functionality, changes to the cryptographic functionality, changes to the audit functionality, profile adjustments, improvements to data transmission to the GWA and additional TOE adjustments.

The evaluation has confirmed:

- PP Conformance: Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014 [8]
- for the Functionality: PP conformant
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.2 and AVA_VAN.5

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
Basic support of integrity, authenticity	SHA-256, SHA-384, SHA-512	[FIPS180-4]	Hash length = 256, 384, 512	TR02102 [17]	2029+
Encryption / decryption, integrity of TSF	AES-XTS-128	[FIPS-197], [IEEE 1619-2007], [SP800-38E]	128 (Enc/Dec), 128 (Integrity)	TR02102 [17]	2029+
Key generation for CMS containers	ECKA-EG	[X.9.63], [RFC3565]	128	TR03116 [16]	2029+
Encryption / decryption /integrity of CMS container	AES-CBC-CMAC	[RFC5652], [RFC6033], [FIPS-197], [RFC4493], [SP800-38A]	128	TR03116 [16]	2029+
Encryption / decryption / integrity of CMS container	AES-GCM	[RFC5652], [RFC5084], [FIPS-197], [SP800-38D]	128 (Enc/Dec), 96 (Integrity)	TR03116 [16]	2029+
Key generation for meter data	AES-CMAC	[RFC4493], [FIPS-197]	128	TR03116 [16]	2029+
Encryption/ decryption, integrity of meter data	AES-CBC-CMAC	[RFC4493], [FIPS-197], [ISO10116]	128	TR03116 [16]	2029+
TLS record encryption	AES-CBC (1)*, (2)* (*cmp. last row)	[RFC5246], [FIPS-197], [SP800-38A]	128, 256	TR03116 [16]	2029+
TLS record layer encryption and integrity	AES-GCM (3)*, (4)* (*cmp. last row)	[RFC5246], [RFC5288], [FIPS-197], [SP800-38D]	128, 256 (Enc/Dec), 32 (Integrity)	TR03116 [16]	2029+
TLS record integrity	HMAC-SHA2	[RFC5246], [FIPS180-4], [RFC2104]	256, 384	TR03116 [16]	2029+
TLS key derivation function	TLS-PRF-SHA2	[RFC5246], [FIPS180-4], [RFC2104]	256, 384 (bit length of PRF)	TR03116 [16]	2029+

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
Integrity of configuration data	CMAC	[SP-800-38B]	128	TR02102 [17]	2029+
TLS-cipher suites	TLS-ECDHE-ECDSA-WITH-AES_128_CBC_SHA256 (1), TLS-ECDHE-ECDSA-WITH-AES_256_CBC_SHA384 (2), TLS-ECDHE-ECDSA-WITH-AES_128_GCM_SHA256 (3), TLS-ECDHE-ECDSA-WITH-AES_256_GCM_SHA384 (4). All cipher suites mandated by TR03116 [16].				2029+

Table 3: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AIS Application Notes and Interpretations of the Scheme

BPL Broadband Over Power Lines

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

CLS	Controllable Local System
CMS	Cryptographic Message Syntax
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
G.hn	Specification for home networking standardised in ITU G.996x
GPRS	General Packet Radio Service
GWA	Gateway Administrator
HAN	Home Area Network
IP	Internet Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
LMN	Local Metrological Network
LTE	Long Term Evolution – Mobile Radio Communication Standard
LTE450	LTE with 450 MHz Frequency
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIM	Subscriber Identity Module
SHA	Secure Hash Algorithm
SMGW	Smart Meter Gateway
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WAN	Wide Area Network
wMBUS	Wireless Meter BUS

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0831-V7-2023, Version 1.7, 2023-10-19, Security Target, SMGW Version 1.3, Power Plus Communications AG

[7] Evaluation Technical Report, Version 3, 2023-11-27, TÜV Informationstechnik GmbH (confidential document)

[8] Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014

[9] Configuration list for the TOE, Version v173, 2023-11-09, EVG-CM-List, Power Plus Communications AG (confidential document)

[10] Handbuch für Verbraucher, Smart Meter Gateway, Version 4.11, 2023-06-02, Power Plus Communications AG

[11] Handbuch für Service-Techniker, Smart Meter Gateway, Version 5.6, 2023-07-05, Power Plus Communications AG

[12] Handbuch für Hersteller von Smart-Meter Gateway-Administrations-Software, Smart Meter Gateway, Version 4.13, 2023-09-01, Power Plus Communications AG

[13] Logmeldungen, SMGW Version 1.3 & 2.1 & 2.1.1, Version 3.4, 2023-05-11, Power Plus Communications AG

[14] Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung, Version 1.4, 2021-05-12, Power Plus Communications AG

[15] Technische Richtlinie BSI TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystem, Version 1.1, 2021-09-17

[16] Technische Richtlinie BSI TR-03116-3, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme, 2022-12-06

[17] Technical Guideline BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths, 2023-01

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 48, Version 1.0, Anforderungen an die Prüfung von Sicherheitsetiketten

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report